APPENDIX A
SECURITY

This appendix discusses the security considerations of the DSRS. Section A.1 provides background information on the sensitivity and classification of the data, and possible system threats. Section A.2 describes each control point, and its vulnerabilities and safeguards within the application. Section A.3 describes the requirements for system monitoring and auditing.

A.1 BACKGROUND INFORMATION. The DSRS is a non-mission critical system. Its primary purpose is to facilitate the potential for cost savings by providing a repository for reusable software. As a result, potential threats to the DSRS can be grouped primarily into the area of data integrity. While confidentiality is a concern, the greatest challenge facing SRP personnel is maintaining the integrity of software objects being reused. The security controls and mechanisms of the DSRS are provided by the operating system, the DSRS application itself, and administrative procedures established by the SRP personnel.

A.1.1 System Security Requirements. Guidance for determining the security requirements for DOD Automated Information Systems (AISs) is provided in DOD Directive 5200.28, *Security Requirements for Automated Data Processing (ADP) Systems* and DOD Directive 5200.1-R, *Information Security Program Regulation*. These policies require all DOD activities to implement a cost-effective AIS Security Program to protect AISs against unauthorized disclosure, modification, destruction, and denial of service. Specific security implementations are contained in the *DSRS Security Plan*, the *DSRS Trusted Facility Manual*, the *Security Feature Users Guide* and the SRP Standing Operating Procedures (SOP). The major goal of the DSRS Security Program is to have the system and network operating at an acceptable level of risk for the Designated Approving Authority (DAA) to grant accreditation. The DAA provided formal implementation of the DSRS on 17 July 1995. To ensure that the DSRS continues to operate at an acceptable level of risk, the DSRS Security Program has established the following objectives:

a. Maintain a high level of confidentiality to prevent unauthorized access to proprietary information;

b. Prevent the misuse of Government computer resources;

c. Protect information from unauthorized modification, which could cause harm to the DSRS, or more importantly, user systems; and

d. Ensure the availability of information to meet customer requirements.

A.1.2 C2 Security Requirements. The computer security requirements for the DSRS were determined by identifying the security operating mode and applying the evaluation criteria presented in CSC-STD-004-85, *Guidance for Applying the Department of Defense Trusted Computer Evaluation Criteria in Specific Environments*. The DSRS currently operates in System High mode, which is defined as a system in which all system users possess clearance and authorization for all information contained in the system. Additionally, DOD Directive 5200.28 requires that all computer

resources that process or handle Classified or Sensitive Unclassified information implement at least C2 functionality (Controlled Access Protection) by calendar year 1992.

A.1.3 C2 Security Requirements Overview. Systems in this class are required to enforce a more finely grained, discretionary access control than C1 systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation. The specific requirements for class C2 protection are provided below with a brief description of each requirement.

a. **Discretionary Access Control.** Restrict access to objects (e.g., files) based on the identity of individuals or defined groups of individuals to protect objects from unauthorized access and to limit propagation of access rights. The controls are discretionary in the sense that owners of data, at their discretion, are capable of permitting others to access data.

b. **Object Reuse.** Eliminate all residual data from a medium (e.g., disk sector) before reassignment of that medium from one subject to another. This prevents users with utility programs from scanning the medium and recovering residual data.

c. **Identification and Authentication.** Identify each individual user of an AIS system before user activity on that AIS system. Establish protective mechanisms, such as passwords, to authenticate the user's identity and to associate all auditable actions taken by that user.

d. **Audit.** Create and maintain an audit trail so that all actions affecting the security of an AIS system can be traced to the responsible party based on individual identity. The AIS system must protect the audit information from modification or unauthorized access or destruction by an unauthorized individual. At a minimum, the following events will be provided by the audit mechanism:

(1) Use of identification and authentication mechanisms;
(2) Introduction of objects into the user's address space;
(3) Deletion of objects from a user's address space;
(4) Actions taken by Computer Operators, System Administrators, and Security Personnel;
(5) All security-relevant events; and
(6) Production of printed output.

The following information is required to be documented by the audit trail:

(1) Date and time of the event;
(2) The unique identifier on whose behalf the subject generating the event was operating;
(3) Type of event;
(4) Success or failure of the event;

(5) Origin of the request (e.g., terminal ID) for identification and authentication events;
(6) Name of object introduced, accessed, or deleted from a user's address space; and
(7) Description of modifications made by the System Administrator to the user/system security databases.

e. **System Architecture.** Create and maintain a domain for execution to protect the Trusted Computing Base (TCB) from external interference or tampering. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

f. **System Integrity.** Provide hardware and software features that will validate correct operation of hardware and firmware elements of the TCB.

g. **Security Testing.** Test security protection mechanisms to confirm their working order as claimed in the system documentation, so that obvious flaws shall be properly identified and corrected.

h. **Security Features Users Guide.** Prepare a section in the user documentation describing the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

i. **Trusted Facility Manual.** Prepare documentation addressing the functions and privileges needing to be controlled when running a secure facility, as well as procedures for examining and maintaining audit files and a detailed audit record structure for each type of audit.

j. **Security Testing Documentation.** Prepare documentation that describes the test plan and results of the security mechanism's functional testing.

k. **Security Design Documentation.** Make available manufacturer's documentation that describes their philosophy of protection and how it relates to the TCB. This document should also include the description of the interfaces between these modules.

A.2 CONTROL POINTS, VULNERABILITIES AND SAFEGUARDS. This section describes each control point, the vulnerabilities at the control point, and the safeguard requirements to reduce the risk to an acceptable level. This description includes consideration of alternate modes of operation based on emergency, disaster, or accident, when appropriate.

A.2.1 Control Points. A control point can be located at any interface where there is movement of data within or between sites. The following control points are considered for this application: input, process, and output.

A.2.1.1 Input Control Points.

A.2.1.1.1 Origin. Data origination controls are used to ensure the accuracy, completeness, and timeliness of data before they are converted into a machine-readable format and entered into the computer application data tables. Controls should ensure that the data reach the application without loss, unauthorized addition, modification, or error. Controls over the data should be established as close to the point of origination as possible, as the remainder of the application processing depends on the accuracy of the source data.

Modification of system edits, required entries, and audit rules should be inaccessible to all users except the local System and Security Administrators.

A.2.1.1.2 System Access/Data Entry. Data input controls ensure the accuracy, completeness, and timeliness of data during their conversion into machine-readable format and entry into the application data tables. The DSRS is unique in that programmer-level users do not directly enter data into the system. Each asset entered into the system is assigned a certification level, which identifies the thoroughness of review by certification personnel. All data entry into the system is accomplished by an authorized Supervisor/Librarian.

a. Password controls should be used to prevent unauthorized access to the system.

b. When keying passwords and authorization codes, non-printing and non-displaying facilities should be used.

c. User access will be disabled, modified, or deleted, as applicable.

d. Documented procedures should be developed to explain the process of identifying, correcting, and reprocessing data rejected by the application.

e. No person should be able to bypass the validation process.

f. Data validation and editing should be performed as early as possible in the data flow to ensure that the application rejects any incorrect transaction before its entry into the data tables.

A.2.1.1.3 Error Correction. Data input errors will be detected and corrected on the data input menu-driven screen.

a. All data entered into the DSRS must be validated at the source of entry. Each data field on the input screen will be subjected to edits that will include alphabetic, alphanumeric, numeric, and verification against tables, ranges, and values, as appropriate.

b. When invalid input is detected, a screen notification and error identification will be displayed on the workstation.

A.2.1.2 Process Control Points. Process controls are procedures designed to streamline transactions to reduce data errors.

A.2.1.2.1 Accuracy and Completeness. The DSRS module will notify the user of the processing success/failure in an on-line message for interactive input.

A.2.1.2.2 System Interfaces. The DSRS interfaces are described in detail in Section 5.4. None of the systems involved are classified. It is assumed that data accepted from other systems will have been through validity edits.

A.2.1.3 Output Control Points. Output control points are the final areas where data accuracy can be monitored. Two output control points occur; they are discussed in the following subparagraphs.

A.2.1.3.1 Production. Production devices authorized to receive output will be determined by the user's access rights. Output devices may be located within a local area network and will consist of various models of both networked printers and local printers. Output will also be provided to exportable magnetic media such as floppy diskette or tape.

A.2.1.3.2 Distribution. The application will distribute output products as an on-line response to a process. Other forms of distribution will be by hard-copy listing or by electronic distribution; both will be generated by the DSRS Librarian after validating receipt of an extract request.

A.2.2 Vulnerabilities. The input of the DSRS application is vulnerable to erroneous input, modification, or deletion of data. Vulnerabilities are discussed by the categories' input control points, processing control points, and output control points.

A.2.2.1 Input Control Points. Vulnerability to unauthorized input, modification, or deletion of data will be controlled by the user's access rights.

a. **Origin**. Vulnerabilities at the point of origin include erroneous information in the input data.

b. **Data Entry**. Librarian error is a vulnerability at this point. Erroneous keystrokes, incomplete information, or other entry errors are types of vulnerabilities encountered.

c. **Disposition**. The loss of source documents prior to verification and correction would have an adverse impact on the accuracy of the application.

d. **Error Correction**. Verification of the accuracy of data used in the correction of input data is required. Although validity edits will be used whenever possible, input of some data is still vulnerable to data entry errors.

A.2.2.2 Processing Control Points. Two processing control points are examined.

a. **Accuracy and Completeness**. One of the critical factors in the effective operation of the application is complete and accurate input data. There must be on-line messages to inform the operator of the success or failure of entering data.

b. **System Interfaces**. Interfaces with other systems have three vulnerabilities:

(1) Potential for processing errors or incorrect data being added to the application,
(2) Possibility of errors being introduced during the transfer process, and
(3) Receiving or target system does not receive the entire input data or the data received are not accurate.

A.2.2.3 Output Control Points. One of the vulnerabilities of a networked configuration is that data could be routed to an unauthorized user. This vulnerability could result in the disclosure of proprietary information to an unauthorized user.

A.2.3 Safeguards. A safeguard is a requirement that will reduce the vulnerabilities at each control point. This section discusses the precautions that can be taken to manage the system vulnerabilities previously described. These include administrative, physical, and technical safeguards.

A.2.3.1 Administrative Safeguards. An administrative safeguard is defined as any procedure that requires management supervision.

A.2.3.1.1 Personnel. Currently, DSRS contains only Unclassified but Sensitive data and, therefore, no security clearance is required for users of the system. Authorization to perform specific functions will be controlled through the user's access rights.

A.2.3.1.2 Collection and Preparation. All data entered into the DSRS will be edited at the source of entry and will be validated against tables, ranges, and values. When invalid input is detected, a screen notification and error identification will be displayed on the workstation.

A.2.3.1.3 Environment Constraints. To provide the assurance that the system will be protected from unauthorized access, the System Administrator will set normal working hours for each user on the system during the process of issuing the new User ID, password, and privileges. These restrictions will be enforced by the system at all times. The System Administrator will also designate a time during non-peak hours that users will not be allowed access to the system, so that backup and maintenance procedures can be accomplished. This will also apply to stand-alone systems. Users will also be required to complete an Account Request Form with a program manager's signature and Non-Disclosure Statement before being issued an account.

A.2.3.2 Physical Safeguards. DODD 5200.28 requires that personnel responsible for Sensitive Unclassified AISs protect hardware, software, documentation, and data from unauthorized disclosure, destruction or modification. Protective means can include personnel, physical, administrative, and configuration controls.

A.2.3.3 Technical Safeguards. Three technical safeguards are examined: user access, process safeguards, and multilevel security requirements.

A.2.3.3.1 User Access. The user must complete an Account Request Form (ARF), which must then be approved by a program manager. The ARF will help control access to the library by requiring authorization of the program manager. Once the ARF is processed, the user will receive a User ID and password. Access to a library system will also be controlled by User ID and password assigned to the user. The user will log in using the User ID followed by the password. If the user does not respond with the correct User ID and password within three attempts, the system will lock the account and require administrator action to reset. Additionally, the server will automatically log off a user after 10 minutes of inactivity. The Librarian will have the ability to assign/deny functional access based on the User ID. The functionality, along with the privileges, will completely define the user's access privileges within a system. It is the responsibility of each DSRS site to establish procedures for processing user accounts.

A.2.3.3.2 Process Safeguards. Whenever feasible, all data entered will be edited at the source of entry and verified against tables, ranges, and values. When invalid input is detected, a screen notification and error identification will be displayed on the workstation.

A.2.3.3.3 Multilevel Security Requirements. The DSRS currently contains only Unclassified but Sensitive (UBS) assets and, as such, there is no requirement for automatic security labeling of subjects (users) and objects (data) in the system.

A.3 SYSTEM MONITORING AND AUDITING. The audit requirements have been identified in paragraph 6.1.3.d and are detailed in the *DSRS Security Plan* and *DSRS Trusted Facility Manual*. The system will provide an audit trail to track system usage and access to RAs on the system. In addition, individual user sessions will generate an audit trail that can be reviewed for errors (i.e., Server log entries).